10:04:59 Seen in the recorded video. And with that out of the way, again, thank you all for, joining EFFs fall members speak easy.
10:05:12 It's great to see so many people in the audience on a Tuesday morning to learn about digital freedoms.
10:05:17 Love to see it. If you're feeling up to it, Maybe let's warm up the chat box.
10:05:23 Feel free to write like where you're from in there. Let everyone know. It's great to see how many supporters are from around the world here.
10:05:34 About twice a year we like to do these member meetups for everyone to learn about digital freedoms, meet some EFF staff, meet some other like-minded folks.
10:05:47 So it's great to see you all here. As just a quick reminder, the reason that we can do this work is because of the support from people like you.
10:05:57 We do this because you're able to donate. Talk to your senators that kind of stuff help us out.
10:06:03 So it's really great to. See the people that make our work possible here. So thank you.
10:06:09 And with that said, we're going to talk about some of the issues EFF has been working on in both the US and around the world surrounding governments justifying increased surveillance and censorship as a way to quote unquote protect the kids.
10:06:24 So today we're gonna invite a couple of staff members to expand on some of the bills we're fighting.
10:06:30 What you can do to push back and, how we can get things right. So first up, I'm gonna introduce, EFF staff attorney, Mario Trujillo.
10:06:40 At EFF, Mario focus on focuses on fourth amendment and privacy rights. He is also part of the coders right project.
10:06:48 Prior to joining EFF, Mario was an attorney at the privacy law firm as well, Jen, and clerked for a federal magistrate judge on the southern border.
10:06:57 And worked as a technology policy reporter at the Hill newspaper. Hello, Mario.
10:07:03 Hey Christian, it's good that everyone's here in the chat. I'm gonna be talking about.
10:07:09 If you know that some constitutional problems with a few state privacy, state child safety laws that have been struck down as unconstitutional.
10:07:19 Let me, bring up my slides.
10:07:24 And so like Christian said, my name is Madio Trujillo. I'm an EFF staff attorney mostly focusing on privacy.
10:07:32 So we're going to talk about a few of these state child safety laws. And so the.
10:07:39 The basic framework is these child safety laws have 2 features to them. One is age verification and the second one is content blocking.
10:07:48 And so it's important to understand how these interact together. And so most of these laws are require a company to verify

the age of their users.
10:07:57 If that user, is determined to be a minor, usually that's a person who's under 17, the laws require the service provider to block certain content for that minor.
10:08:11 That's either by restricting that minor from accessing the product at all or it's giving that minor a diminished product.
10:08:21 So it's a social media platform with, some harmful content removed. And so It's a one way to look at it is age verification is kind of the mechanism that enables the the platform to sensor or block content.
10:08:39 And so we'll talk about each one of those. And so what are the problems with age verification?
10:08:45 First, it's important to understand, what type of age fair, we're talking about that it goes from sort of least invasive to most invasive to most invasive.
10:08:54 And so at the least invasive to most invasive to most invasive. And so at the least invasive you've probably seen, of least invasive to most invasive.
10:08:58 And so at the least invasive, you've probably seen a button that requires you to test that you're either over at the age of 13 or over the age of 17.
10:09:03 More invasive than that is. A button that requires you to enter your birth date more invasive than that is.
10:09:12 A requirement that a platform, verify your age through government ID, either a passport or a driver's license.
10:09:20 And even more invasive than that is a. Recording or a screen capture of your face in order to run it through a biometric algorithm for the algorithm to estimate the age of a person based on their facial facial geometry.
10:09:37 And so each one of those has inherent problems, but they all kind of have these 4 problems within them.
10:09:44 And so the first one is privacy and security. And so by implementing an age gate and age verification system especially in age verification system that requires government ID, you're sort of eliminating one of the the initial sort of bargains that the internet is that, you can browse the internet anonymously.
10:10:05 The second problem is that. Hey, DATA verification systems require data. And so that's data that a technology company can either reuse or resell or re purpose for some other use.
10:10:20 It's important to remember that a lot of these laws have restrictions on what the tech company or the the platform can do with that that age verification data but you know you're putting your data in the hands of a extra data in the hands of the technology company in your, you know, sort of relying on them to do.
10:10:40 To do what's right. So one, there's bad actors who might misuse that data.
10:10:47 There's also, threats of data breaches, you know, and that, no law can really protect you from a data breach.
10:10:54 And so sometimes the best use restriction is just a, collection restriction. Next, there are speech concerns and the speech

concerns overlap with privacy concerns and so under the US First Amendment, there is a right to access and distribute data anonymously, the age verification systems obviously would I hinder that, especially age verification systems that require government IDs.
10:11:22 It, they also, These age verification systems would also deter both adults and children from accessing certain content.
10:11:32 And so certain content that is either a embarrassing or sensitive, a person might not want to have their name associated with that search term.
10:11:41 Or that's that query. And so that's going to deter both the adults and children from accessing that content.
10:11:48 There's also a second deterrence is that some privacy conscious people won't want to make that bargain that you know I want to read this news article but I don't want to give up my personal data to do it and so that's also going to be a deterrence from allowing people to access certain content.
10:12:05 Moving down the list to discrimination this is mostly in the context of age verification systems that require a government ID.
10:12:16 First off many children don't have a government ID you know i didn't i grew up in a small town and i didn't travel a lot and so I didn't get a passport until I was 18.
10:12:28 I didn't get a driver's license until I was 15 or 16. And so that eliminates a swath of children that don't have a government ID.
10:12:37 More than that though, even there's certain populations of the, of it ended up adult population that don't have a government ID ID.
10:12:46 That's the other. Focused in low income areas or in the undocumented community and so that would either eliminate those people from accessing platforms in general or create extra barriers for them to.
10:13:00 Access the platform. And then finally there are accuracy issues and this is specifically in regard to the age estimation through biometric collection.
10:13:10 This is a new technology that's not perfected and it's questionable whether it could ever be perfected but at the current state.
10:13:19 Age estimation can be off by a year or 2. And so when you're trying to Identify a 16 year old compared to an 18 year old, you know, you're gonna have a lot of mismatches.
10:13:32 So that's going to be either over inclusive or under inclusive. So that's the first, those are the problems with age verification.
10:13:38 The second, thing is what, what's the problem with content blocking? I won't spend a lot of time on, problems with content blocking because they seem pretty self evident.
10:13:48 You know, if you enact a law that requires. Platforms to block a certain harmful content to children, they need to open up an age gate that is going to diminish, the platform for both adults and children alike.
10:14:04 If you put up a age gate and you serve children a diminished

project product based on a you know a a product that has Hold on harmful content removed.
10:14:18 That's gonna sweep up a lot of protected content even that children have a first amendment right to access children have a you know they have maybe diminished First Amendment rights but they do have First Amendment rights to access content and so a lot of the the laws are written in a vague terms to block or sensor harmful content and sometimes that that term harmful can you know be anything it doesn't sometimes
10:14:48 they're written to maybe block pornography but they're written in a way that it blocks all sexual content.
10:14:55 And so. That's gonna be. Limiting children from, from accessing certain protected content.
10:15:03 And then finally, children aren't a monolith. It's a lot of these laws are written to, to stave off.
10:15:11 Harms to minors and that's you know it's sort of they minor is anyone below the age of 17 usually and so what is theoretically harmful to a minor might not be old what's theoretically harmful to an 8 year old might not be harmful to a 13 year old might not be harmful to a 16 year old and so one of the key features of these laws that
10:15:36 have major problems is they treat children you know all from 0 to 16 as a sort of one unit that has a So the same sensibilities.
10:15:47 And so how is this played out on the ground? There's already been. 3 court cases that have 3 courts have issued injunctions which is just a temporary block.
10:15:59 Of 3 of these child safety laws, one in Arkansas, one in Texas and one in California.
10:16:05 So the one in Arkansas. It's requires age verification usually through government ID and if a person is determined to be a minor, they are blocked from the social media platform except with parental consent.
10:16:21 In Texas. The age verification system worked for, for online platforms that had a certain amount of sexual content.
10:16:31 If that platform determines that a child's, or that person is a minor, the person is completely blocked from that website.
10:16:41 But the, you know, the term sexual content is very vague and it's over inclusive and it, you know, it can.
10:16:47 Range from everything anything to from obscenity which is unprotected to pornography which is protected to you know, sort of a Just to maybe a risque, photo or something like that.
10:17:00 And so those 2 laws were struck down. Mostly because of the age verification. The courts said that.
10:17:09 One, it's going to prevent adults from accessing. Protected speech because they're going to be deterred from from entering.
10:17:17 Those platforms and then 2 even when the age verification works. And children. You know, are blocked from certain content.
10:17:26 They're going to be blocked from, content that they have a constitutional right to access. The California law is a little different in that it strongly encourages age estimation and so that is the would likely be the technique of a biometric phase scan.

10:17:43 And that age estimation does 2 things. One, it requires companies to, block certain content to it would actually give children a privacy protections that would sort of be the lever to give children privacy protections.
10:18:01 And so at EFF, we believe that age gate. Would be unconstitutional and it would sort of, that's the way to implement both the content blocking and the the privacy provisions and while we like Some of the privacy provisions even.
10:18:17 Yeah, if they wouldn't have been sort of tangled up in this age verification system and content blocking system.
10:18:25 You know, those privacy provisions are things we would like in a privacy bill, but when you, Use an age verification method like, you know, age estimation to implement that, that we think that, That's not gonna, that's not gonna withstand.
10:18:41 First Amendment scrutiny. And so those are 3 laws that right now have been blocked. There are 2 other laws one in Texas and then a pair of laws in Utah which will likely suffer the same fate and in the next couple months and you know to the extent more and more states are passing these laws or.
10:19:02 At the federal government more. Congress or the Senate passes these laws. They're likely gonna suffer the same fate, of just being struck down.
10:19:12 The Arkansas, Texas and California law are up on a peel, but, as they stand now, they're on hold.
10:19:19 And then, so what's the solution? I think. Here at EFF, we think that strong data privacy legislation can be a solution.
10:19:29 And I think it does 2 things, these child safety laws can't do. The first one is that data privacy legislation has a strong track record of being upheld by the courts as constitutional just to take 2 examples the federal wiretapping laws have been around for about a hundred years.
10:19:53 The Supreme Court has called, HIPAA, which is a, data privacy law that regulates health data a a smart law, a, And so other laws have also been upheld.
10:20:09 It's constitutional as data privacy legislation. So it's it's just data privacy legislation is better equipped to survive these court challenges.
10:20:20 The second big thing is that data privacy legislation actually gets at one of the root causes of what people perceive as ills online and that's a.
10:20:31 Sort of a surveillance apparatus that is. Meant to serve and deliver targeted ads. And so one of our key priorities is to ban behavioral advertising.
10:20:42 And you add a data minimization and then you add a Strong. Enforcement mechanisms. We think that gets at a lot of the problems that.
10:20:53 These child safety laws are trying to address in a sort of censorship regime. We think that data privacy legislation gets at that.
10:21:05 In a more straightforward manner.

10:21:08 And so finally, I'm gonna sort of pivot. I've been talking about state laws.
10:21:15 These are laws that have been enacted by states that were about to go into effect. That got struck down by the courts, but there are also federal proposals.
10:21:24 Bills that are being debated in Congress and in the Senate that have many of the same problems, though not identical problems.
10:21:32 And one of these bills is called the Kids Online Safety Act. Short name is KOSA.
10:21:38 The Senate, this week is trying to use a procedural move to, pass COSA by unanimous consent and we have we've put up an action alert to have our members Call and.
10:21:52 Voice their concerns to their senators. We have a action page at EFF. If you just, type in COSA, you'll find the action alert.
10:22:01 And so we urge you, you all to spend 5 min today and call your senator if you're in the United States and ask them to not not RAM through this this dangerous child safety.
10:22:15 And so I think that's it for me and I will hand it back to Christian. I'm happy to answer questions at the end.
10:22:23 Thank you, Mario. That was really great and super interesting to learn about. We'll do Q&A's for Mario at the end of Mario. That was really great and super interesting to learn about.
10:22:35 We'll do Q&A's for Mario will transition to EFF seniors free speech but let me restart EFF senior speech and privacy activist page callings at EFF page focuses on fulfillment of civil liberties and corporate threats to speech and privacy online.
10:22:53 Page has worked with governments and activists across the globe to collaboratively facilitate change. Welcome page and excited to hear what you got to talk about.
10:23:02 Thank you so much and thank you everyone for joining us today. I think we're so excited to to talk about this issue which is transcending boundaries across different countries.
10:23:12 And an issue with so pervasive to kind of argue again. So like Mario, I'll be sharing some slides.
10:23:19 Again, if you have any questions, please do. Put them in the chat and we'll end up to answer them at then.
10:23:27 So. Here we have the Uk's online safety bill which is a really big piece of legislation. It's now unfortunately the online safety act.
10:23:39 So I should enter. It's now the online safety act and I'll talk you through how that came to be and I'll talk you through how that came to be and why that came to be and why we're frustrated with it.
10:23:47 Essentially, how that came to be and why we're frustrated with it essentially. So, you know, we just asked us now the kids online safety, all the different legislation in the US, COSA, we have here early.
10:23:56 When we think about these topics you might wonder why we care. Why is this such a big privacy issue?
10:24:01 And I think essentially it comes down to one thing, which is

that at our core, we all have the right to private conversation and to determine when we want to share information with our loved ones, with our family members, with our friends, and when that happens, who hears it.
10:24:16 And the moment and the mechanism upon which we we communicate that and a bunch of these pieces of legislation really erode on that right.
10:24:22 And you know, in the human rights framework, that's protected under the right to privacy in lots of national and international mechanisms on human rights.
10:24:31 But, it's really about choosing those moments and these bills kind of take away from that. And unfortunately, we're seeing at them in many places.
10:24:39 So, Mario discussed the different pieces of legislation in the US but unfortunately we're seeing it in many places so Mario discussed the different pieces of legislation in the US but unfortunately we also have the online safety bill.
10:24:49 So Mario discussed the different pieces of legislation in the US. So Mario discussed the different pieces of legislation in the US, but unfortunately we also have the online safety bill, now the Online Safety Act in the US, but unfortunately we also have the online safety bill in the US, but unfortunately we also have the online safety bill, now the online safety act in the United Kingdom.
10:25:08 We have the child sexual abuse with protecting encryption but unfortunately with the online safety act we don't have that kind of trajectory so it's been a long process working with the online safety act.
10:25:15 First it was emerged in 2,017 as the internet safety strategy green paper. And this strategy between paper emerged on the back, unfortunately, of a young girl in the UK who It was exposed and saw more than thousands of people, thousands of pieces of self-harm content in the weeks leading to her unfortunately ending her life.
10:25:38 When that happened, the government decided to attempt to take action to make the online space as you can see here the safest space in the world to go online and help shape an internet that is open and vibrant.
10:25:52 But also protects its users from harms. A big claim you could say, but that was essentially the goal and that's where we're at.
10:26:01 So in 2,022 the online safety bill was introduced following as you can see here in many years of consultations.
10:26:08 Under its fourth prime minister, the online safety act passed just a few weeks ago at the end of October.
10:26:16 It's changed a lot since the Internet Safety Strategy Green Paper. That was pretty targeted as a green paper.
10:26:23 It had very kind of specific goals and asks pertaining to children's rights online as I mentioned emerging from the back of the young girl that lost her life or took her life in 2,017.
10:26:35 And the bill that we ended up with. Is certainly very different to that. Kind of, so we look at kind of what we've been working on with EFF actions and the online safety bill.

10:26:55 There were 2 kind of what we've been working on with EFF actions and the online safety bill.
10:27:00 There were 2 kind of big focus areas that we've been working on with EFF actions and the online safety bill, there were 2 kind of big focus areas that we really orient in our work towards.
10:27:04 The first was provision, And this piece of this They should, you know, like the online safety bill is 260 plus pages.
10:27:10 It sought to contain everything, you know, a, PPPP, pornographic content to doxing, to enter an encryption to clients, to doxing, to enter an encryption to clients that mandating clients like scanning so it was extremely broad and in this you know there were lots of different issues but the first one was that legal but harmful provision and that essentially you sought to
10:27:30 criminalize any content that's definitely legal but was harmful so it might be insulting or inflammatory.
10:27:36 This was illegal. This is an illegal provision. Under the UK and European and international law, you can communicate content that's either, you know, shocking, offensive, insulting and that comes actually from a court case that happened in the UK hand-decide versus United Kingdom.
10:27:55 So That was a kind of one of the big core issues and we were working with coalitions, we submitted a consultation at a briefing to the consultation.
10:28:03 And last year that Persian was removed from the online safety bill so of course you were thinking great this is fantastic the online that this legal but half of provision has been removed and things are just up from here, soon we'll get the end of the bill.
10:28:18 But unfortunately once that provision was removed by the government they decided to go fully committed to eroding the right to end-to-end encryption and so that's kind of how our focus oriented in lobbying on this piece of decision.
10:28:30 There were many clauses specifically close 1 10 which subsequently changed a number of different causes, which sort to mandate client side scanning.
10:28:39 Of the credit with accredited technology and that accredited technology would be accredited by the government and the Uk's regulator. Ofcom.
10:28:48 So all of this is very insular. Of course, we probably all know in this call you cannot have a technology that just is supposed to scan for a child's educational material or harmful content.
10:28:59 A black door for one is a black so for all it's quite simply a fundamentally impossible and incompatible to have a piece of, you know, technology that can scan for one thing and and not everything.
10:29:11 So we were trying to make this argument and I think I know what Mario was saying is this is such a polarizing issue.
10:29:18 And I think what Mario was saying, it this is such a polarizing issue, we were saying, this is such a polarizing issue.
10:29:20 We were talking lots with politicians, we held briefings, we were communicating with them on why this was such a problematic piece of legislation, we held briefings, we were communicating with them on

why this was such a problematic piece of legislation and specifically this clause monitoring private messages.
10:29:33 And many of them were saying, you know, maybe I agree, you know, I agree definitely, but I don't want to take that position publicly because I have to be seen as protecting children online.
10:29:42 And if I don't support this bill, it seems like I'm not protecting children online.
10:29:47 We were able to kind of get to a stage towards the end of the bill where there was a massive coalition of security researchers, cybersecurity experts, politicians, we had a number of different apps, Google, Signal, Meta, or many of the encryption apps as well and services, Apple saying this piece of legislation is terrible, most of them saying it if it does willing to be of ourselves from the UK market because
10:30:11 we're not prepared to undermine encryption by, you know, complying with this with this legislation.
10:30:16 We also held a private briefing in the House of Lords. Things, you know, and there was a big commitment, but unfortunately it seemed like it was 1, 1, 65 for many of these people in the house of peers in the House of Lords, which they were not prepared to take this stand, you know, they were they were very much communicating that they were in favor but.
10:30:36 It was too much of a risk, a political risk for them to defend encryption, which ultimately in the discourse meant not caring about children's rights.
10:30:45 So the bill passed. Here's one of the amendments you were trying to to edit, you know, you can say leave out privately.
10:30:55 So we'll go through this for a long time. In the end the bill passed a few weeks ago as I mentioned, but not all hope is lost.
10:31:01 So specifically with this bill that makes it quite different to many other pieces of legislation in the UK and internationally really is that it can't been printed overnight.
10:31:13 So the bill itself is contingent on Ofcom implementing and creating and then implementing codes of conduct and guidelines and rules of practice.
10:31:19 To implement this bill. So, The next stage and this will take years because as I mentioned there bill is 260 pages plus long every single provision needs to be converted into an operational piece of legislation that that can be introduced.
10:31:36 So Ofcom last week introduced their first guidelines. It's nearly a thousand pages long. So we've got a lot of reading ahead of us working on this bill.
10:31:44 But it will be step by step so they've communicated that next year they'll be trying to seek to tackle the issue of encryption.
10:31:51 And in that we've got a lot of capacity for influence. They're reaching out civil society.
10:31:55 We had a private meeting with them last week and a number of our civil society politicians. We're in contact with them building out the this piece of legislation into something that can be operationalized into the law.

10:32:07 So that's kind of one thing, building out the this piece of legislation into something that can be operationalized into the law. So that's kind of one thing.
10:32:18 So it's not definitely, you know, it Second is litigation so maybe you're thinking this can't be legal.
10:32:21 Maybe it's not I think there are lots of litigation options when we go forward. You know, we've got article 8 on the right to privacy, the right to private life on the European Convention.
10:32:31 So that's one possible avenue of being able to take a specific component of this legislation to perhaps a judicial review in the United Kingdom or to the European Convent through the European Convention rights to European courts arguing that I could, illegality and legitimacy of this piece of legislation.
10:32:51 And the campaigning side, so one of our colleagues is in London tomorrow for a meeting with signal and a number of civil society organizations to really discuss this this piece of legislation in the next step.
10:33:03 So what can we do in our coalition? What can we do as EFF to make sure that the bill doesn't get get implemented essentially, you know, how can we stop this?
10:33:12 How can we at an injunction or how can we advocate for people to recognise their rights before it even happens.
10:33:17 So I think what's really interesting is that not all hope is lost. We've we've actually got a period of time now where because the bill cannot be implemented straightaway, we can really frame the language and discourse that's going to be going to be introduced.
10:33:29 And I think when we like other pieces of legislation, for example, the CASA, the regulations against child sexual abuse in the EU.
10:33:41 We are experiencing wins and so this is not an issue where the discourse is finalized and there is no chance of permeating through that.
10:33:48 You know, it was mentioned in the chat already, but this piece of the, this regulation coming out of the EU is pretty much a same as coast. It's the same as online safety bill.
10:33:57 It's just that it's attempting to stop the distribution of known content. Actions against huge content, it has a detection order and of course introduces hindsight scanning as a preference.
10:34:08 Today, so this is new. Information as of today, we reached a compromise deal. So following, you know, more than 70 organizations working across the EU and Europe, working on this piece of this on this file in the European Union, we're able to reach a compromise by the European Parliament.
10:34:27 Here are a few of the big winds, so no MASS scanning, which is a huge one.
10:34:32 The scanning must be targeted with a specific suspicion. With judicial oversight, so unlike the Uk's online safety act, which has no judicial oversight or parameters on the use of accredited technology.
10:34:42 This is very specifically targeted. Grooming detection is removed from the scope of detection orders and I think within this

parameter what was really interesting about this regulation is that the EU wanted to introduce AI to detect any harmful content on text messages or in emails.
10:35:01 And so removing that and having judicial oversight is really beneficial. Another is a, you know, protection at anti encryption which would be in screaming at the European Union to protect for a long time so private messaging apps cannot be subjected to any scanning technology.
10:35:14 A for vacation as Mario discussed it at length earlier, no mandatory age verification for private messaging and absolute as well as safeguarding it.
10:35:22 You can, you know, hear, hear about web crawling in Europol and then also blocking orders.
10:35:31 So even now it's restricted, this is about web crawling in Europol and then also blocking orders.
10:35:33 So even now it's restricted, this is still problematic, you know, it made possible on hosting services.
10:35:34 So we reached a definitely a beneficial compromise based on months and months of advocacy at EFF and in a wider coalition.
10:35:41 And the next steps, are you making what's next? So this will now go to the European Council.
10:35:48 And where they will discuss that position which is is not necessarily known at this point. But there's selection in the Open Union next year and so if there's no compromise that can be met between the institutions, the file could get stuck.
10:36:03 So we're going to keep the pressure on for a good final deal for consumers, but people in the European Union and I think we can take this this win here as an indication and a recognition that whilst we're fighting these bills, there there is you know there are challenges here you can see some some actions you know we're part of these campaigns.
10:36:18 Raising awareness here is for a football match you know stop chat control. Edd you know European digital rights network have been coordinating this so it's really fantastic since the initiative.
10:36:33 And here is just, I thought, you know, we're talking today about. You.
10:36:35 S. Bills and and UK and Europe and Harry kind of all the lines in one picture which is essentially we've got people like Ashton Kutcher, you know, he, as of course, Clap, but coming to your European Union and being able to talk in in different chambers and institutions about this bill to protect the children.
10:36:55 But I would be, you know, big emphasis kind of to conclude this presentation is. We know that this these bills introducing clients I have scanning, eroding the rights to end to end encryption and undermining technology is not only not protecting the children, but it's in deep putting them at further risk of harm, especially guns that rely on encrypted communications and private channels the most.
10:37:15 So we'll continue doing that. You know, the UK, there's a lot of potential now to mold the implementation of the Online Safety Act and in the EU to really push for a final resolution that backs up

today's win.
10:37:29 Thank you so much.
10:37:34 Cool. Thank you so much, Paige. That was great. I think, yeah, we got Mario back up too.
10:37:40 So now, we've got some time to answer some of the audience questions that were coming up in the chat.
10:37:45 So I think we'll just get started. This first one came from Kagan, which who said, would it make sense if we somehow all agreed on using a separate a separate trusted party.
10:38:02 That would only provide this sort of ruling required age 16 meets age true slash false. Normally I oppose eliminating it, but I doubt this issue will go away.
10:38:14 Did you either if you all have thoughts?
10:38:16 Yeah, so I think that's Sorry, I think that question. Is at that question comes up in the context of age verification and the question is, you know, if we move.
10:38:28 This age verification to a trusted third party rather than the tech company. Does that make it safer?
10:38:35 I think that that just moves the liability without eliminating the risk. And so instead of, you know, who's got that information, it's some third party that is unknown and maybe less trusted and so that could you know it could pose even more concern.
10:38:51 That is unknown and maybe less trusted. And so that could, you know, it could pose even more concerns in case we don't or trust that company.
10:38:55 It can also, I think it, creates sort of a large, honey pot for, data breaches.
10:39:03 And so I think that rather than fixing the problem, I think it just moves the problem. But all the, all the concerns still remain.
10:39:15 Thanks for that. Next up, this one comes from, Augusto? I was just wondering, are laws assigning you unique identifier numbers to babies at birth a common thing around the world or is it just Brazil?
10:39:31 That certainly makes it easier for companies to track, track children's data and build dossiers of their behavior since birth.
10:39:39 Nowadays, you can't do anything in Brazil without a kid's CPF number.
10:39:45 I'd be there. We all, heard about that.
10:39:46 Yeah, so I can talk about that from a US perspective. And so all, Everyone in the United States has a social security number, the social security number was originally set up to give benefits to people at the at the end of their retirement.
10:40:07 I think the social security number in the United States is a good example of a of a survey. Identifiers slash data collection regime that was meant for a very normal or a very narrow set of circumstances that has really exploded into this not not a universal identifier in the United States, but it's definitely taken on a lot more prominence than.
10:40:31 Than what it was designed for and because of that, the social security number is very, unsecure and, it has led to a lot of, financial fraud and so i think yet i think at least in the united

states that is that's the thing I haven't heard of proposals that propose using a social security number or a social security hard as the form of age
10:40:57 verification, but I, if, If an age verification system is asking for a government ID, I guess that.
10:41:04 That could be one of the methods used, but I don't think that that is a. I don't think that's something that lawmakers are proposing.
10:41:17 Cool. I think this next one will be for, you, with the recent passing of the online safety bill, do we expect to see messaging apps and services, do we expect to see messaging apps and services withdraw from the UK?
10:41:33 And what would that look like?
10:41:33 That's a great question. Thank you for asking it. Specifically because in the weeks leading up to the online, the final vote of the online safety bill in the House of Lords, a number of messaging apps and services decided to public, say that they would leave the UK market if the online safety bill passes, which indeed it now has.
10:41:52 The rationale of those proclamations is that they don't want to undermine end to end encryption.
10:41:58 On their sites and on their services and platforms and therefore the cost of compliance is too high and I think this point is interesting because there's a criminal liability and introduced in the online safety act for noncompliance with the provisions under this bill.
10:42:12 So. Yeah, managers, meta, for example, or signal if they don't comply with this bill, can be imprisoned.
10:42:20 They will also be fined extensively for non-compassing 14%. So it's very, very high amount of money.
10:42:25 Fund and compliance of the annual turnover. And so when if you want to be services and now we're talking about tier one types of so big services if you're one of these these companies and so big services if you're one of these these companies and corporations you've got the these companies and corporations you've got the European Union where you have provisions and legislation and files to comply with and then you have the UK Online Safety Act which almost
10:42:46 contradicts many of those and if you're working within all these countries it's perhaps Nonsense call to uphold the Online Safety Act when you've got 27 other countries in the European Union and a stronger risk of noncompliance for with those pieces of legislation.
10:43:03 So I think it's left the, you know, in private conversations with some of these services, they have told me we're still very committed to upholding into an encryption. They have told me, we're still very committed to upholding into an encryption.
10:43:15 We don't want to leave. It's certainly the last last option, but we still very committed to upholding into an encryption. We don't want to leave.
10:43:19 It's certainly the last last option, but we still will if we can't reach a compromise on how the bill is implemented, and

specifically on the technology that is supposed to be accredited to mandate client-side scanning.
10:43:26 You know, we've got a declaration in the week before the online safety bill passed that the government recognized that right now the technology doesn't exist to scan for child sexual abuse material or harmful content and not scan for everything else which was a win because they refused to acknowledge that in 2,017.
10:43:45 But, I think it's left to be seen. I hope that some of these corporations, indeed all of them, hold their word and and do leave the UK market.
10:43:53 But of course, that 60 million people will be losing out and it's not just people in the UK.
10:43:56 It's people communicating with those in the UK. You know, some of these encrypted apps are used by, you know, people who are seeking asylum and they're in detrimental situations coming out and they need to communicate for a safe passage into the UK.
10:44:07 Or for human rights defenders sharing information from one country at risk to to maybe somebody in the UK. So it's not just people in the UK that will miss out.
10:44:17 So I really hope that we can find a solution before these services have to make the United Kingdom.
10:44:25 Cool. Thanks for that. This next one's really interesting.
10:44:30 And something I've thought about before, from Grady. See Sam is such an emotional issue that excuses the entire framing of the issue.
10:44:39 The issue is at the forefront to get people to accept surveillance that they otherwise wouldn't. How can this framing be challenged?
10:44:45 Surely overblocking is also harmful to children.
10:45:00 So good.
10:44:54 Did I either of you guys have thoughts on challenging the framing for See, Sam.
10:45:00 Yeah, I don't know if I can talk, sorry. But we actually found this, in the chat control.
10:45:09 And the reason was that later in the game, the Europe policy critically inserted their own, phrasing.
10:45:18 Like one paragraph or so where they basically said like any police can use this data so you should probably look for something like this because I would bet would be there as well.
10:45:32 Okay, that's
10:45:37 Hey, did you wanna say something?
10:45:40 Yeah, thank you so much, Andrew, for sharing that. And indeed, I think this is probably the biggest issue is tackling this narrative.
10:45:47 This discourse is so pervasive, it's so paramount. None of us don't want children to be protected, but by eroding their rights online, they are at more risk.
10:45:57 I think it comes from a number of different angles and I've seen in the chat some conversations about how can we fight against the discourse of I've got nothing to lose so I don't mind an invasion of

my privacy rights and I think it's about reorienting that framework to recognize that we do have these right so it's not about what's to lose but it's I have these and
10:46:16 it's something to gain when we think about face surveillance for example it's face recognition is maybe one of the most lovely things ever you know when you see somebody that you know after a long time on the street or if you're you're going home for the holidays and you see your family members and your friends that's what face recognition should be used for it, should it be used to scan our faces and surveillance without
10:46:35 our consent and I think we can take that same approach into messaging services we have these rights to privacy so we can communicate with our loved ones the information that we want to and when we want to and we know when that's going to be taken and not just for us but for the profits of big corporations and so restructuring that and trying to tackle it from a different angle because I think it can get really tricky also I
10:46:55 think we've shown this many times. I go into another, but we have the right to priority.
10:46:59 It's like, I don't have anything to lose. It's like, I don't have anything to lose.
10:47:03 Children need protections. They have rights to they need anonymous channels and I think what's been super frustrating about these bills is especially in the UK is that a lot of the advocates for the bill have also anonymous channels that children can report abuse or bullying or so they recognize that children do need anonymous channels to to report the harms against them but apparently not online.
10:47:22 So there's that I think so finally there's a much bigger issue which is that just because a child experiences harm online doesn't mean they're not experiencing harm offline and they're whatever happens online is not in a vacuum and so really building out frameworks for children to feel safe both online and offline.
10:47:38 In a broader community holistic framework is also one approach to tackling that.
10:47:48 I'm muted, sorry. Did you have anything to expand Mario or did Page cover at all for you?
10:47:53 Well, so yeah, the bills that I, I outlined are less about, filtering and blocking CSM, but there are proposals in the United States, you know, that, in in this filtering and blocking would also create liability or could create liability for end-to-end encrypted apps.
10:48:15 Those are I'm thinking of proposals like the Ernest Act or the St. Act. And I think one of the one of the answers to that is not to preframe the issue in that, you know, CSAM is despicable and it should be stopped.
10:48:29 It's that law enforcement, at least in the United States, law enforcement has tools right now to, to address that.
10:48:37 There, are laws that create liability if if tech companies don't report CSAM when they have actual knowledge to my knowledge that

has never been a law that's enforced.
10:48:51 That, sort of outlaw the promotion of that kind of material and that law is also, Not enforced and so.
10:49:02 I think one answer is to ask why, you know, why these lawmakers are.
10:49:07 Pushing these new proposals when they have enforcement tools and one of the one of the answers is for them to strengthen their enforcement of existing laws rather than creating new laws that create a lot of different problems and create a lot of uncertainty for end to end encrypted apps that like page said offer a lot of value and protection encrypted apps that like page said offer a lot of value and protection in and of themselves.
10:49:36 Cool. Thank you. This next one, comes from Ben.
10:49:42 I'd be curious to get y'all's perspective on the practical enforceability of potential client side scanning slash end to end.
10:49:50 Provisions. Thinking less about the mega tech companies and more about every project uploaded to GitHub that provides encryption and whatnot.
10:49:59 If the implications that every, OSS, I think that means open source. Project going to pull from some mandatory repository.
10:50:11 Do you all have thoughts on that question?
10:50:18 So.
10:50:17 Maybe from the UK.
10:50:23 No, no, you go ahead.
10:50:24 Okay, I think, maybe taking the first part of the question about the enforceability of client side scanning, something that we try to emphasize in the UK and across the EU with with stop chat control is that.
10:50:37 You know, it's not possible to protect rights and implement client-side scanning without, those rights.
10:50:46 It's just fundamentally incompatible to have privacy and erosions on end to end encryption.
10:50:49 So it's not enforceable. It's a and I think that's the thing that we've tried to emphasize in the UK specifically, which is that the technology that the government have consistently said over the last 5, 6 years is eggs are sick, you know, exists as possible.
10:51:07 We can, we can scan for CSAM and other harmful content, which is also really a subjectively defined briefing list of topics and subject to change.
10:51:16 We can scan for clients. We can scan for that and not scan for anything else. We can only use our technology and no other technology as possible.
10:51:24 I think what we've tried to emphasize at each stage of that is it's not possible to enforce that without opening it up for everything else.
10:51:29 So you have a back door for the government. With their credit technology, you're then opening it up for hackers for for rogue states, for harmful actors.
10:51:38 To expose and take advantage of that. And, and in doing so, it's, it's, for, this privacy rights, unenforceable, but it didn't

marry if you have a different elucidations on that.
10:51:48 No, I'll leave it there.
10:51:53 Cool. I think that we have a time for a few more questions. This is one, that's been on my mind that I think you could answer Mario.
10:52:04 You talked a bit about, like a more consumer privacy laws as a way to fix some of these issues.
10:52:12 So a lot of states including California already have privacy laws. Would a federal law replace these state laws or how would that work?
10:52:21 No, no, so, the What EFF has advocated for a long time one of the one of the key pillars of a federal data protection law would be that it does not override state laws.
10:52:36 And so that has that along with the, the consumer enforcement, provision has been a large sticking point, but we think, any federal privacy law should be sort of the floor of privacy in the United States and not the ceiling.
10:52:52 And so if California which has been a leader in privacy legislation in the United States wanted to increase those privacy protections we think that's that's a good idea I think that's Going back to the sort of the purpose of the state and federal government states have have always been seen as sort of a laboratory for different laws.
10:53:15 Different and improved laws and those sort of filter up to the federal level. And so I think any privacy law that.
10:53:24 That gets enacted at the federal level, we we would. Push very hard to make sure that that's the floor and not the absolute through ceiling of what privacy protections in the United States look like.
10:53:40 Cool. Thank you. And,
10:53:46 For page. How could the online safety bill affect other social media and child safety efforts in, Europe?
10:53:55 So the online safety act has age verification. So like Mario explained, I won't duplicate because it's almost exactly the same.
10:54:08 There, I won't duplicate because it's almost exactly the same. There are provisions within this bill that are trying to prevent children from seeing content that's almost exactly the same.
10:54:15 There are provisions within this within this bill that are trying to prevent children from seeing content that's within this bill that are trying to prevent children from seeing content that are trying to prevent children from seeing content that are trying to prevent children from seeing content that's, you know, for example, pornographic, but again, harmful, which is pretty subjective.
10:54:21 And it's requiring blocking children from, you know, children from viewing these, these websites in sight.
10:54:25 So not only is it trying to scan for content but it's blocking children or those underage of using certain sites and I think you know, children are very innovative.
10:54:36 It's not just having these build is not going to prevent children from viewing these platforms and it's it's a an incorrect

solution to a problem that we've we've been trying to communicate for a long time now.
10:54:46 So what happens in the UK we've mentioned so many times I think it's probably going to be a blueprint for similar builds around the world given that it's almost the first it's kind of have passed in such a way which has such erosions on client side of encryption through client side scanning.
10:55:05 And probably we'll see duplications or at least now a commitment from other countries to Echo that I've heard that whilst I've spoken to governments around the world and that you know the UK have this pass in the UK so it's kind of involved in the them a lot of legislation but in that sense we just continue to fight back and as we want had you know have this win today a broad coalition of organizations in the European Union
10:55:28 been really fighting for the CISA regulation, a broad coalition of organizations in the European Union been really fighting for the CC regulation.
10:55:39 So not all hope is lost and I think we can try and replicate those, strategies elsewhere and really make sure that you know the children that it can access you know have device to access the online world are safe but it in the way that we know best access the online world are safe, but it in the way that we know best and not by, preventing them from accessing certain websites and apps and by, in the way that we know best and not
10:55:50 by, in the way that we know best and not by, preventing them from accessing certain websites and apps and by
10:55:52 Okay, I will just quickly ask since I lost like, where in the, but I can tell you like in a very short, 5 min, are very short how we went to the you parliament with a and how it worked and maybe the reason how we want so maybe something you could reimplement or.
10:56:15 You use for your environment. If you want, I don't know if it's this, if this, if this, until 8 or how much time do we have.
10:56:29 I think we were close to, wrapping up, but I don't. I don't know if, Page Mario wanted to hear or if you wanted to like shoot us a note@infoateff.org.
10:56:41 Everyone here can shoot us a note there and we go through all the emails and check those too.
10:56:48 And I think you can you can also go on stop scanning us or you go on the entry website, the grouping digital rights.
10:56:57 As just being mentioned, and you can find the campaign their calls stop scanning. That's Scott's going.
10:57:02 And you can and you can find out that and that given the the news today and the win today in the European Union, given the news today and the win today in the European Union, you'll probably see lots on the EFF website in the coming days and different social media channels as well to hear that.
10:57:16 But, please do follow up on that because it's a really good win in the landscape of pretty dire legislation.
10:57:20 So we want to amplify that and share that. This legislation and these types of legislation. Can be, can be challenged and we can

win and we want to replicate that in as many places as possible.
10:57:38 Cool. And so with that, I think it's time to close out. So thank you.
10:57:45 All for joining again and thank you Paige and Mario for presenting answering some questions. It was really great to hear from you all.
10:57:53 And also just another reminder, thank you all for joining and, for being EFF supporters.
10:58:01 Like I said at the start, the reason we're able to continue this work is because of your continued support.
10:58:08 And if you know you're here and you haven't donated yet this year, we'd love to have you.
10:58:14 Stay on as an EFF member. You can donate@eff.org size join.
10:58:19 And if you have any questions for us, please send a note after, info at EFF.
10:58:23 Dot org. But, until then, thank you guys so much and, we'll see you at the next one.